1. Login Window bằng tk notadmin/notadmin
2. Chạy BeRoot

A screenshot of a computer program

AI-generated content may be incorrect.

1. Xem kết quả với BeRoot

Ta thấy BeRoot cung cấp cho chúng ta 1 dịch vụ có tên VideoStream có đường dẫn không được trích dẫn

1. Chạy PowerUp.ps1

A screenshot of a computer screen

AI-generated content may be incorrect.

1. Xem kết quả với PowerUp

PowerUp cung cấp cho ta 1 vài thông tin hữu ích

* Đường dẫn ko được trích dẫn của dịch vụ VideoStream
* 1 số lỗ hổng DLL hijacking trong thư mục %PATH%
* 1 số lỗ hổng liên quan đến quyền và thực thi dịch vụ

1. Xem qua dịch vụ VideoStream trên trang của dịch vụ

A screenshot of a computer

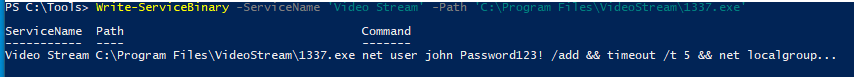
AI-generated content may be incorrect.

Có thể thấy được đường dẫn ko được trích dẫn trong dấu “”

1. Khai thác lỗ hổng bằng PowerUp

**Write-ServiceBinary -ServiceName 'Video Stream' -Path 'C:\Program Files\VideoStream\1337.exe'**

* Write-ServiceBinary: là 1 function trong PowerShell được sử dụng để tạo 1 dịch vụ mới và cung cấp tệp thực thi cho dịch vụ đó
* ServiceName: tên dịch vụ bạn tạo
* Path: đường dẫn đến tệp dịch vụ



1. Khởi động lại máy tính và xem kết quả

A blue screen with white text

AI-generated content may be incorrect.

A blue screen with white text

AI-generated content may be incorrect.

Thành công tạo tài khoản john với quyền Admin.